UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/824,595	04/02/2001	Randall Scott Springfield	RPS9 2000 0016	1231

7590   08/05/2004

I. B. M. Corp., Intellectual Property Law
Personal and Printing Systems Group
Dept. 9CCA/Bldg. 002-2
P.O. Box 12195
Research Triangle Park, NC 27709

EXAMINER
GYORFI, THOMAS A

ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 08/05/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

	Application No.	**Applicant(s)**
Office Action Summary	09/824,595	SPRINGFIELD ET AL.
	Examiner	**Art Unit**
	Tom Gyorfi	2135

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) FROM
THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed
  after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any
  earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is
closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-12* is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-12* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage
application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date *4/2/01*.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____.

1.   Claims 1-12 have been examined.

Claim Rejections - 35 USC § 102

2.   The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that

form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act

of 1999 (AIPA) and the Intellectual Property and High Technology Technical

Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting

directly or indirectly from an international application filed before November 29, 2000.

Therefore, the prior art date of the reference is determined under 35 U.S.C. 102(e) prior

to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

3.   Claims 1, 4, 6, 7, 9, and 11 are rejected under 35 U.S.C. 102(e) as being

anticipated by Grawrock (U.S. Patent 6,678,833).

Regarding claim 1, Grawrock discloses a method of protecting boot block data

and accurately reporting boot block contents. In the invention disclosed by Grawrock, a

boot block memory unit (element 220 of Figure 2) loads upon startup of a computer

platform (element 100 of Figure 1) and records an identifier into a memory location

(element 330, Figure 3) contained within a Trusted Program Module (TPM: element 230

of Figure 3; method: element 410 of Figure 4). The identifier is created by means of a

cryptographic operation, either by digital signing or by hashing (column 2, lines 35-46).

Next, the boot block memory locates and loads the BIOS for execution; a BIOS identifier

is then similarly recorded. During the computer's normal operation, the TPM is

available for inquiry requests from unspecified challengers, either internal or external to

the computer platform. The TPM can respond to valid requests with a digital signature

featuring the boot block identifier, keying material, certificates, and the like (column 4,

lines 10-18). This is understood to mean that the boot source used by the processor

during a given system boot can be determined. Furthermore, in one embodiment of the

invention disclosed by Grawrock, the boot block identifier can be recorded into non-

volatile memory on the first startup of the platform, and then the value can be retained

for use in subsequent startups (column 3, lines 62-67). This is understood to mean that

the boot source is specified once as a known boot source.

Regarding claim 4, again note that the invention disclosed by Grawrock writes

the boot block identifier and the BIOS identifier (the boot sources for the platform) into

special memory locations inside the TPM (column 4, lines 25-30).

Regarding claim 6, the invention disclosed by Grawrock contains a processor

(element 110 of Figure 1) and a boot source comprising a boot block unit (element 220

of Figure 2) and a BIOS (element 340 of Figure 3). The processor and boot source are

coupled together via a bridge comprising a memory control hub (MCH) and an I/O

control hub (ICH) as illustrated in Figure 1. The ICH is connected to a packaged IC

device (element 150) containing a boot block memory unit and a Trusted Program

Module via a link (element 160, Figure 1). Inside the Trusted Program Module is a

memory that contains a boot block identifier and a BIOS identifier. As noted previously, the boot block identifier can be embodied in such a way as to have the identity of the boot block be written once, and stored for subsequent startups (column 3, lines 62-67). Therefore, the boot block identifier is understood to be equivalent to the second register that allows the boot source to be specified once as a known boot source. Similarly, the BIOS identifier is understood to be equivalent to the first register that stores an identity of the boot source used by the processor each time the computer system boots.

Regarding claim 7, as noted above the processor and boot source are coupled by means of a bridge comprising the MCH and ICH units (Figures 1 and 3). It should be noted that in one embodiment of the invention disclosed by Grawrock, the MCH and ICH are integrated into a chipset together, thus functioning as one component (column 3, lines 7-9). In addition, the Trusted Program Module containing the boot source identifiers is connected to the ICH (element 160 of Figure 1). Grawrock teaches that in one embodiment of this invention, the packaged IC device containing the TPM may be employed within the ICH, thus incorporating its functionality into the ICH directly (column 3, lines 18-24). In that embodiment, the memory containing the boot source identifiers would be located within the bridge.

Regarding claim 9, again note that the boot block identifier can be embodied such that it is written only once to the appropriate memory location, and the value stored therein is retained for use in future startups (column 3, lines 62-67).

Regarding claim 11, again note that the BIOS identifier is written to the
appropriate memory location in the TPM each time the computer system boots (column
4, lines 25-30).

Claim Rejections - 35 USC § 103

4.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all
obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set
> forth in section 102 of this title, if the differences between the subject matter sought to be patented and
> the prior art are such that the subject matter as a whole would have been obvious at the time the
> invention was made to a person having ordinary skill in the art to which said subject matter pertains.
> Patentability shall not be negatived by the manner in which the invention was made.

5.   Claims 2, 3, 5, 10, and 12 are rejected under 35 U.S.C. 103(a) as being
unpatentable over Grawrock as applied to claims 1, 6, and 9 above, and further in view
of Angelo (U.S. Patent 5,944,821).

Regarding claims 2 and 10, Grawrock does not explicitly teach that the boot
source is a flash boot source. However, Angelo teaches a computer system having a
flash ROM containing the BIOS information (Angelo, column 7, lines 30-34). It would be
obvious to one of ordinary skill in the art at the time of the invention disclosed by
Applicant to utilize a flash ROM containing the BIOS in the invention disclosed by
Grawrock. This would allow an authorized user to reprogram the BIOS with relative
ease so as to accommodate future revisions of the BIOS.

Regarding claim 3, as noted above the flash ROM disclosed by Angelo contains
BIOS information, but not necessarily information regarding the boot block. However,
Grawrock teaches that it is possible to embody his invention in a manner such that the

entire BIOS may be substituted for the boot block code (Grawrock, column 3, lines 40-47). Thus, it would be obvious to one of ordinary skill in the art at the time of the invention disclosed by Applicant that one could substitute the identifier for the Flash BIOS in place of the boot block identifier. Since it has already been established that the memory location for the boot block identifier can be designated as a write-once memory location (Grawrock, column 3, lines 62-67), the Flash BIOS identifier can then be written once into memory and identified for future boots. Doing so adds extra security by including a potential means for detecting boot block tampering that cannot itself be tampered with.

Regarding claims 5 and 12, Grawrock recites that the method disclosed in his invention is unable to detect modifications to information regarding the boot process (column 1, lines 45-48). However, Angelo discloses a method by which programs are registered for execution in secure memory contained in a computer system by means of hash identifiers stored in a hash table. For each program that is to be registered, an identifier is generated through a hashing algorithm and stored in a hash table in secure memory (Angelo, column 9, lines 3-12). Note that the means to generate an identifier are equivalent between the two patents (Angelo, column 9, lines 35-45; Grawrock, column 2, lines 40-46). When a user wishes to execute a program on the computer system as disclosed by Angelo, a hash signature of the program in its present form is generated, and the computer system compares it to the stored hash signature of the program as it was registered. If the signatures match, the program is allowed to run (Angelo, column 10, lines 16-26). Therefore, it would be obvious to one of ordinary skill

in the art at the time of the invention to incorporate the act of comparing two hash

values for equality as disclosed in Angelo into the system disclosed by Grawrock.

Recall that the BIOS identifier can be used in place of the boot block identifier, as noted

in the rationale for rejection of claim 3. Thus, one of ordinary skill in the art at the time

of the invention could store the known value of the BIOS in the boot block identifier

memory location and current value of the BIOS in the BIOS identifier memory location.

It would then be obvious to one of ordinary skill in the art at the time of the invention to

compare the contents of those two memory locations at startup to verify that the current

boot source is the known boot source. In this manner, one can detect modifications to

information regarding the boot process, thus correcting a known flaw in the invention

disclosed by Grawrock and also providing for a more secure computer platform.

6.   Claim 8 is rejected under 35 U.S.C. 103(a) as being unpatentable over Grawrock

as applied to claims 6 and 7 above, and further in view of the articles "VIA's New South

Bridge: VT82C686B Supporting UltraATA/100", by Patrick Schmid, published October

26, 2000 (henceforth "the VIA article"); and "Intel Pentium III i815e Motherboard

Shootout", by Mickey Sethi, published December 8, 2000 (henceforth "the Pentium

article").

        The term "south bridge" does not appear in the text of the Grawrock patent;

however, Grawrock discloses an I/O controller hub, or ICH, that communicates with

peripherals attached via a PCI bus, USB bus, or ISA bus (column 3, lines 10-17). The

VIA article teaches that a south bridge, as typically understood by one of ordinary skill in

the art, controls various peripherals including I/O ports and USB devices (page 2,

paragraph 1, "Chipsets Basics"). In addition, it teaches that at the time the invention by

Applicant was made, the Intel Corporation had elected to discontinue the use of the

north and south bridge nomenclature in favor of the terms MCH and ICH (page 2,

paragraph 3, "Chipsets Basics"). Corroborating this teaching is the Pentium article,

which explicitly teaches that the ICH is a direct equivalent to a south bridge (page 1,

paragraph 4, "Introduction"). Thus it is self-evidently obvious to one of ordinary skill in

the art at the time of the invention that an ICH can be substituted for a south bridge as

specified in Applicant's claim.

Conclusion

7.   The prior art made of record and not relied upon is considered pertinent to

applicant's disclosure.

- U.S. Patent 5,537,540 (Miller et al.), "Transparent, Secure Computer Virus

  Detection Method and Apparatus";

- U.S. Patent 5,421,006 (Jablon et al.), "Method and Apparatus for Assessing

  Integrity of Computer Software";

- "Super Video Graphics Array Support by Notebook PC", IBM Technical

  Disclosure Bulletin Volume 37, Issue 6B, pages 71-72, 06/01/94.

8.   Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Tom Gyorfi whose telephone number is (703) 308-4954.

The examiner can normally be reached on 8:00am - 4:30pm Monday - Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Kim Vu can be reached on (703) 305-4393. The fax phone number for the

organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the

Patent Application Information Retrieval (PAIR) system. Status information for

published applications may be obtained from either Private PAIR or Public PAIR.

Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see http://pair-direct.uspto.gov. Should

you have questions on access to the Private PAIR system, contact the Electronic

Business Center (EBC) at 866-217-9197 (toll-free).

TAG - 07/27/2004
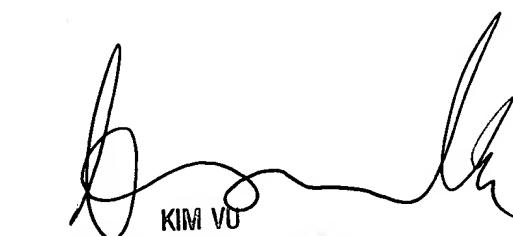
KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100